

FILED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
(Alexandria Division)

2012 APR -5 A 11:33

-----X
TECH SYSTEMS, INC.,

Plaintiff,

CLERK US DISTRICT COURT
ALEXANDRIA, VA 22314
Index No: 1:12-cv-00374-GBL
JFA

-against-

LOVELEN PYLES and JOHN AND JANE DOES 1-10,

Defendants.

-----X

COMPLAINT

Plaintiff Tech Systems, Inc. (“Tech Systems”), by its undersigned counsel, for its Complaint against defendant Lovelen Pyles (hereinafter “Defendant” or “Ms. Pyles”) and John and Jane Does 1-10 (collectively the “Defendants”), alleges upon information and belief as follows:

NATURE OF ACTION

1. Tech Systems is a federal government contractor with numerous contracts with the Department of Defense and other federal agencies. Some of those contracts provide work to the Department of Defense in critical areas of defense.
2. From October 17, 2011 through April 2, 2012, Defendant Pyles was Tech Systems’ Human Resources Manager. During that time, she used her position to gain valuable information regarding Tech Systems’ computer systems, employee records, and customer information.
3. Prior to and after her termination, Ms. Pyles has engaged in a campaign of harassment and destruction aimed at terrorizing Tech Systems’ management and

employees, destroying Tech Systems' relationship with its customers and overall business. She has done so through illegal and unlawful means. To wit, by: revealing personal human resources information company-wide, physically disconnecting Tech Systems' computer systems (which were housed in a secure area of Tech Systems' corporate office and connected to the internet), accessing her e-mail after being terminated and sending confidential information out to unauthorized recipients, changing the boot-up sequence for Tech Systems' computer systems thereby rendering it inaccessible, attempting to access private data regarding Tech Systems' employees including their social security numbers, and sending threatening text messages to Tech Systems' employees.

4. Ms. Pyles' thirst for revenge has been raging for four days and there is no sign of it being quenched until Tech Systems disintegrates and all of its employees are out of work necessitating this emergency relief.

JURISDICTION

5. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. §§1331 and 1338 because questions of federal law have been presented under 18 U.S.C. §1030, *et seq.*

6. Additionally, this Court has diversity jurisdiction pursuant to 28 U.S.C. §1332(a)(1) because: (i) the parties are diverse with Plaintiff's principal place of business in Virginia and Defendants located in Maryland; and (ii) the amount in controversy exceeds \$75,000.

7. This Court also has supplemental jurisdiction over Tech Systems' state law claims pursuant to 28 U.S.C. §1337.

8. This Court has personal jurisdiction over the Defendants pursuant to Va. Code §8.01-328.1 because the place of the claims alleged in this Complaint took place in Virginia.

9. In addition, venue is appropriate in this Court pursuant to 28 U.S.C. §1391 because a substantial part of the claims arose in this district.

THE PARTIES

10. Plaintiff Tech Systems is a Virginia corporation having its principal place of business at 6420 Grovedale Drive, Suite 300, Alexandria, Virginia, 22310.

11. Defendant Pyles is a resident of the State of Maryland with an address of 10014 Tallahassee Place, Waldorf, MD 20603. She is a former employee of Tech Systems and worked at Tech Systems' corporate office located at 6420 Grovedale Drive, Suite 300, Alexandria, Virginia, 22310 from October 17, 2011 through April 2, 2012.

12. Defendants John and Jane Does 1-10 are acquaintances of Defendant Pyles whose true identities are not yet known. However, each of the John and Jane Does 1-10 are persons, who by virtue of their association with Pyles, were able to commit, or to aid and abet in the commission of the acts set forth and complained of herein. The identities of John and Jane Does 1-10 can not be ascertained at this time.

FACTS COMMON TO ALL CLAIMS

A. **TECH SYSTEMS**

13. Tech Systems is a Woman-Owned, Small Business Government Services Contractor located in Alexandria, Virginia that focuses exclusively on Government customers, providing a high level of professional service.

14. Tech Systems has more than 30 years of expertise managing personnel to perform a variety of outsourced operations in areas of national critical importance. More

specifically, Tech Systems currently has contracts to provide services at: (i) the Bulk and Retail Mobility Fuel Supply Point, National Training Center and Ft Irwin, CA; (ii) the Weapons Field Training Battalion, Camp Pendleton, CA; (iii) the School of Infantry, Camp Pendleton, CA; (iv) the United States Geological Survey, Earth Resources Observation and Science (EROS) Center, Sioux Falls, SD; (v) Lackland Air Force Base, TX; (vi) the Joint Readiness Training Center and Ft. Polk, LA; and (vii) the Marine Corps Station, Parris Island, SC; (viii) the U.S. Coast Guard Academy, New London, CT; and (ix) Fort Eustis, VA.

15. Three of the contracts listed above require Tech Systems to possess a Secret Security Clearance.

16. Tech Systems' Executive Team includes two (2) licensed Certified Public Accountants (CPA) and a licensed attorney who bring uncompromising professionalism, integrity and dedication to all of their contracts.

B. PYLES' TENURE AT TECH SYSTEMS

17. On October 11, 2011, Defendant Pyle was hired by Tech Systems to be its Human Resources Manager. Ms. Pyle reported directly to Anne P. Rohall, Esq., Vice President and General Counsel.

18. Upon commencing work at Tech Systems, Defendant Pyles agreed in writing to abide by certain Tech Systems' policies contained in its employee handbook (the "Handbook").

19. Relevant to this dispute, the Handbook¹ contains the following:

**CONFIDENTIAL INFORMATION AND CONFLICT OF
INTEREST**

¹ In the Handbook, Tech Systems is defined as "TSI."

General Confidentiality Obligations

Information that pertain to TSI business, including all nonpublic or proprietary information concerning the Company, its vendors and suppliers, is strictly confidential and must not be given to people who are not employed by TSI.

Please help protect confidential information – which may include, for example, trade secrets, customer lists and company financial information – by taking the following precautionary measures:

- Discuss work matters only with other TSI employees who have a specific business reason to know or have access to such information.
- Do not discuss work matters in public places.
- Monitor and supervise visitors to TSI's contract locations to ensure that they do not have access to confidential information.
- Destroy hard copies of documents containing confidential information that are not filed or archived.
- Secure confidential information in desk drawers and cabinets at the end of every business day.

Your cooperation is particularly important because of our obligation to protect the security of our Government clients' and our own confidential information. In addition, if you work on a classified contract or at a classified facility, there are additional standards that apply to you and they will be communicated separately. Use your own sound judgment and good common sense, but if any time you are uncertain as to whether you can properly divulge information or answer questions, please contact the Corporate office.

Employee Privacy and Other Confidential Information

TSI collects only personal information about employees that relates to their employment. Only people with a business-related need to know are given access to this information. The Company President and CEO must authorize any release of the information to others. Personal information, other than that required to verify employment or to satisfy legitimate investigatory or legal requirements, will only be released outside the Company with advanced employee consent.

If you have access to any confidential information, including private employee information or confidential Company or Government information, you are obligated to act with integrity. Unauthorized disclosure or inappropriate use of confidential information will not be tolerated.

Account Transactions

Employees responsible for handling or disbursing funds must assure that all transactions are expected and authorized...

Account and Customer Information

Employee[s] are prohibited from distributing confidential account, client, and/or customer information to anyone, in any form, except to the named account holder, client or customer.

Compliance

Employees who fail to comply with this policy will be disciplined, which may include a demand for reimbursement of any losses or damages, termination of employment and/or referral for criminal prosecution. Action appropriate to the circumstances will also be taken against Supervisors or other who fail to report a violation or withhold relevant information concerning a violation of this policy.

20. Tech Systems also has a Computer and Software Usage Policy that is part of the Employee Handbook. This Policy contains the following provisions, in relevant part (with emphasis added):

Use of Company Communication Systems

The communication and information systems at Tech Systems, Inc. and at Government worksites should be used only for conducting Company business. Communication systems include, but are not limited to any handheld wireless device such as palm organizers, laptops and Blackberries or more traditional devices such as phones, fax machines and mailing systems. Information systems include computers, internet/intranet networks and email.

Since Tech Systems, Inc. reserves the right to access any personal communications without prior notice, Company and Government-provided systems should not be used by employees to transmit any messages or to access any information that they would not want to be viewed or heard by a third party.

Incidental, occasional and infrequent use of the Company's or Government's communication and information systems for personal use is permitted as long as such use does not interfere with your work or the work of any other employee or with the computer's operations.

The communication and information systems of Tech Systems, Inc. or the Government may not be used for any illegal, unethical, destructive or wasteful purpose. Employees

should exercise in personal use of any communication and information systems device. Employees should not expect personal information stored in these systems to be kept private.

21. This Policy also emphasizes the fact that corporate e-mail is the property of Tech Systems and may only be used for business purposes.

22. The following is Ms. Pyles' agreement to comply with the terms of Tech Systems' employee handbook:

I understand that I must comply with all of the provisions of the Employee Handbook. I also understand that if I do not comply with all provisions of the Handbook, my access to Company resources may be revoked, and I may be subject to disciplinary action up to and including termination of employment.

I further understand that I am obligated to familiarize myself with the Company's safety, health, and emergency procedures as outlined in this Handbook or in other documents.

10/17/11
Date

Lorellen Pyles
Signature

Lorellen Pyles
Please Print Your Name

*Please sign, date and return this page, along with your other employment documents, to
TECH SYSTEMS, Inc. at toll free fax: 1-888-788-4169*

53

23. Ms. Pyles' tenure at Tech Systems was marked by insubordination and poor work product. For instance, on multiple occasions, Ms. Pyles sent out letters to clients and employees that contained incorrect information, typographical errors, and poor grammar. Ms. Rohall discussed these issues with Ms. Pyles on multiple occasions, but to date, these problems were not corrected by Ms. Pyles.

24. Further, Ms. Pyle was exceptionally defensive when given constructive criticism. Often times, she would send sarcastic e-mails following a session that was meant to correct a poor attitude or work product.

25. Most recently, Tech Systems learned that one of its contracts was being insourced by the Government. Because of that, some employees who were working on the contract would be losing their jobs. As is its custom, Tech Systems was going to send letters to these employees thanking them for their service to the company. Ms. Pyles was tasked with that assignment and sent out the letters to the employees losing their jobs. The letters, however, contained multiple errors including the wrong contract information, incorrect name spellings, incorrect tenure with the Company and incorrect addresses, as well as numerous spelling mistakes infuriating Tech Systems' outgoing staff.

26. On Friday, March 30, 2012, Ms. Rohall met with Ms. Pyles to discuss this issue and again set up a remediation plan that required Ms. Pyles to pass all outgoing correspondence with a supervisor.

C. MS. PYLE'S CAMPAIGN OF DESTRUCTION

27. In the early hours of Sunday, April 1, 2012, Ms. Rohall received a series of e-mails from Ms. Pyle complaining about her treatment at Tech Systems and sarcastic references to Ms. Rohall's abilities as a manager.

28. An example is below,

-----Original Message-----

From: Lovelen Pyles [mailto:lovelen.pyles1@verizon.net]
Sent: Sunday, April 01, 2012 1:52 AM
To: Anne Rohall
Subject:

Hi Anne

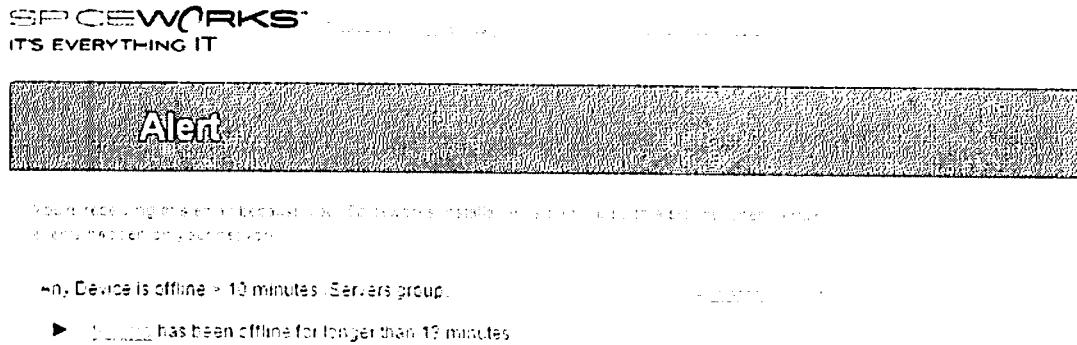
I was up working and saw your message. My blackberry is acting crazy!! I thought the horse was still alive because it was brought up. I thought our culture was to be fair and respect each employee. And if I've done something wrong, I would be told right then and there. But if the horse is really dead it will not be discussed again.

I was just shocked my errors made the company get laughed at and not what Larry said to the world we have no policies in place. Or check issues from finance. I know I missed up big time and so have others. They were never told the company is being laughed at due to their errors.

I agree the horse is officially dead. I'm soooooo glad I can discuss my feelings with you. See you on Monday.

29. Thereafter, on Sunday evening, Jose Andrade, Tech Systems' Director of Operations and Technology received an electronic notification that Tech Systems' server was down. The e-mail is below:

From: Spiceworks Desktop on DirOpsTech DirOpsTech@tsi-corp.com
Sent: Sunday, April 01, 2012 8:28 PM
To: jandrade1@tsi-corp.com
Subject: ts1-corp has been offline for longer than 13 minutes



30. Mr. Andrade tried to log onto the server remotely to diagnose the problem, but was unable to do so.

31. When employees began arriving on Monday, April 2, they discovered that the main server and the finance server, e-mail and internet access were all down and the Company's label printer and postage printer were also not functioning.

32. Mr. Andrade, along with Ms. Rohall began investigating the source of the outage and discovered that:

- a. Someone compromised the secure server room at Tech Systems' offices and physically disconnected many of the components; and
- b. Someone had accessed the finance server and changed the BIOS boot-up information and altered the start-up sequence so that it would not load properly.

33. Only a few employees have access to the secure access room. One of those employees was Defendant Pyles.

34. Immediately, Tech Systems launched an internal investigation to determine who had sabotaged the server and finance server, both of which are connected to the Internet, and concluded that Ms. Pyles was the perpetrator.

35. Simultaneously, Tech Systems was attempting to limit the damage from being completely disconnected from its clients and workforce and for not having access to its own internal records. To that end, a team of employees spent hours trying to diagnose the various problems caused by the acts of sabotage and correct them. This, naturally, prevented all of these employees from doing their regular work

36. In the evening of Monday, April 2, Tech Systems President and CEO, Nancy Blethen, called Ms. Pyles to ask for her resignation. Ms. Blethen told her that unless she resigned, she was terminated. Ms. Pyles became irate at this ultimatum. By phone the next day, Tuesday, April 3, Ms. Blethen reiterated to Ms. Pyles that she was terminated.

37. Further, Tech Systems contacted the Fairfax County Police, which is investigating this matter.

38. Tech Systems is also in the process of retaining a private investigator and has retained Centre Law Group to bring this action to help them prevent further acts of sabotage through consultation and the instant action.

39. The unlawful and illegal actions did not end there.

40. Following Tech Systems' termination of Ms. Pyles, she engaged in a campaign to damage Tech Systems' business.

41. *First*, after she was fired, but prior to the time her e-mail was disconnected, Ms. Pyles utilized Tech Systems' corporate e-mail (which she was no longer permitted to access) to e-mail sensitive personnel information to employees and others not authorized to receive such information. For instance, she e-mailed out a

confidential e-mail from the corporate office discussing whether a particular employee should be fired to that employee. She also e-mailed a memorandum that an employee had sent to the corporate office in confidence to others within the company who were the target of that memorandum.

42. *Second*, after she was fired, but prior to the time her e-mail was disconnected, Ms. Pyles utilized Tech Systems' corporate e-mail (which she was no longer permitted to access) to inform Tech Systems' field employees that she was unjustly terminated.

43. *Third*, after she was fired, Ms. Pyles left numerous messages on Tech Systems' phone voicemail box system in an attempt to harass Tech Systems and/or render the voicemail system useless.

44. *Fourth*, after she was fired, Ms. Pyles attempted to access Tech Systems' online benefit account as an administrator on at least four occasions. As an administrator, she would be able to view all of the employee's personally identifiable information such as social security numbers, dates of birth, addresses, etc.

45. *Fifth*, Ms. Pyles has sent offensive e-mails and text messages to current employees causing at least one employee to stay home from work because of the stress associated with the current situation created by Ms. Pyles.

46. Finally, while Tech Systems conducted a background check of Ms. Pyles prior to the time she was offered a position at Tech Systems, Tech Systems has now conducted a more thorough investigation of Ms. Pyles. Said investigation has revealed (i) a new civil action against Ms. Pyles filed last week; (ii) domestic abuse charges and a restraining order against Ms. Pyles for violent behavior; and (iii) a previous arrest for drinking while intoxicated.

47. Ms. Pyles' past history coupled with her actions herein have left Tech Systems no choice but to seek emergency relief from the Court and has left Tech Systems' employees and owners fearing for their personal safety.

48. To date, it is unclear whether Ms. Pyles is acting alone or has enlisted the aid of an accomplice. Tech Systems plans to determine the identification of possible accomplices through discovery.

COUNT I

**VIOLATION OF THE COMPUTER FRAUD
AND ABUSE ACT, 18 U.S.C. §§1030, ET SEQ.
AGAINST ALL DEFENDANTS**

49. Tech Systems repeats, reiterates, and re-alleges each and every allegation as contained in the previous paragraphs with the same force and effect as if fully set forth herein at length.

50. As demonstrated in the conduct described above, Defendants intentionally accessed Tech Systems' computer systems without authorization and/or Ms. Pyles' access to Tech Systems' computer systems exceeded her authorized access. This is especially true (but not limited to) instances where Ms. Pyles accessed her corporate e-mail after she was fired and accessed the finance server to change the BIOS start-up information.

51. The computers and systems accessed by Ms. Pyles were protected computers as defined under the Computer Fraud and Abuse Act.

52. Ms. Pyles' access of Tech Systems' computer systems caused damage to said system and was made with an intent to defraud in a manner that affects interstate commerce.

53. Ms. Pyles' access of Tech Systems' computer systems caused enormous monetary damages to Tech Systems including, but not limited to, fees being paid to investigators and attorneys who have investigated this matter and are helping Tech Systems prevent further unauthorized intrusions. Because Tech Systems possesses a SECRET facility clearance, every breach must be taken seriously and costs the company an enormous amount of money and time.

54. Further, Tech Systems' work to fix the problems caused by Ms. Pyles and the lost working hours from unproductive employees due to a lack of access to Tech Systems' critical systems cost Tech Systems an enormous amount of money.

55. Tech Systems has also had to necessarily contact the Fairfax County Police Department to report these incidents.

56. At a minimum, Tech Systems has been damaged in an amount of at least \$30,000 in direct damages attributable to Ms. Pyles violation of the Computer Fraud and Abuse Act. In addition, Ms. Pyles' actions are causing irreparable harm to Tech Systems.

COUNT II

BREACH OF FIDUCIARY DUTY **AGAINST DEFENDANT PYLES**

57. Tech Systems repeats, reiterates, and re-alleges each and every allegation as contained in the previous paragraphs with the same force and effect as if fully set forth herein at length.

58. As the head of human resources for Tech Systems entrusted with confidential and proprietary information and trade secrets, Ms. Pyles owed a fiduciary duty to Tech Systems.

59. Ms. Pyles breached those duties by engaging in the acts described above.

60. As a proximate cause of Ms. Pyles' actions and wrongful conduct, Tech Systems has suffered and continues to suffer substantial damages including loss of productivity from its staff tasked with fixing its computer system and investigating the sabotage, possible defections of employees who are expensive and time consuming to replace, and a loss of good will and reputation among its partners, employees and customers. While difficult to quantify and growing by the day, said damages are at least \$75,000.

61. Ms. Pyles' conduct is outrageous, intentional, and exhibits a high degree of moral culpability. As such, Tech Systems is entitled to an award of substantial punitive damages.

COUNT III

BREACH OF CONTRACT **AGAINST DEFENDANT PYLES**

62. Tech Systems repeats, reiterates, and re-alleges each and every allegation as contained in the previous paragraphs with the same force and effect as if fully set forth herein at length.

63. Ms. Pyles agreed to the terms contained in the employee handbook, which created a contract.

64. Her actions described in detail above violated the provisions of the Employee Handbook excerpted above.

65. By virtue of Ms. Pyles' actions and wrongful conduct, Tech Systems has suffered and continues to suffer substantial damages including loss of productivity from its staff tasked with fixing its computer system and investigating the sabotage, possible defections of employees who are expensive and time consuming to replace, and a loss of

good will and reputation among its partners, employees and customers. While difficult to quantify and growing by the day, said damages are at least \$75,000 in addition to the irreparable harm Tech Systems is suffering.

COUNT IV

VIOLATION OF THE VIRGINIA COMPUTER CRIMES ACT **AGAINST ALL DEFENDANTS**

66. Tech Systems repeats, reiterates, and re-alleges each and every allegation as contained in the previous paragraphs with the same force and effect as if fully set forth herein at length.

67. Defendants have used a computer network or computer without authority and obtained property by false pretenses, embezzled, or committed larceny, and/or converted the property of Tech Systems in violation of the Virginia Computer Crimes Act, Va. Code Section 18.2-152.3 *et seq.*

68. By virtue of Defendants' actions, Tech Systems has suffered substantial damages (greater than \$75,000) and continues to suffer irreparable harm.

COUNT V

TRESPASS **AGAINST ALL DEFENDANTS**

69. Tech Systems repeats, reiterates, and re-alleges each and every allegation as contained in the previous paragraphs with the same force and effect as if fully set forth herein at length.

70. Tech Systems maintains password protected computer systems.

71. Without permission or authorization from Tech Systems, Defendants entered upon these protected computer systems including servers and e-mail and took possession (and disseminated) said information.

72. By virtue of Defendants' actions, Tech Systems has suffered substantial damages (greater than \$75,000) and continues to suffer irreparable harm.

COUNT VI

**MISAPPROPRIATION OF TRADE SECRETS
UNDER THE VIRGINIA UNIFORM TRADE SECRETS ACT
AGAINST ALL DEFENDANTS**

73. Tech Systems repeats, reiterates, and re-alleges each and every allegation as contained in the previous paragraphs with the same force and effect as if fully set forth herein at length.

74. Tech Systems maintains numerous trade secrets and proprietary information internally including the contact information of its customers and employees, financial information, and SECRET information.

75. Ms. Pyles misappropriated said information and unlawfully disseminated it to numerous other people without Tech Systems' permission or authorization.

76. By virtue of Defendants' actions, Tech Systems has suffered substantial damages (greater than \$75,000) and continues to suffer irreparable harm.

COUNT VII
**VIOLATION OF TITLE II OF THE
ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §§2701, ET SEQ.
AGAINST ALL DEFENDANTS**

77. Tech Systems repeats, reiterates, and re-alleges each and every allegation as contained in the previous paragraphs with the same force and effect as if fully set forth herein at length.

78. Tech Systems maintains on-site servers for corporate files, accounting records, email and internet access. These servers constitute “facilit[ies] through which [] electronic communication[s are] provided” within the meaning of 18 U.S.C. §§2701 *et seq.*

79. Ms. Pyles intentionally accessed, without authorization, such facilities, or otherwise intentionally exceeded her authorization. Through this access, she thereby obtained, altered, and prevented others from having authorized access to a wire or electronic communication while it was in electronic storage.

80. By virtue of Defendants’ actions, Tech Systems has suffered substantial damages (greater than \$75,000) and continues to suffer irreparable harm.

WHEREFORE, Plaintiff demands:

- a. An award of monetary damages in the amount of \$30,000 under Count I of the Complaint;
- b. An award of monetary damages in the amount to be determined at trial of not less than \$75,000 under Counts II III, IV V, VI, and VII of the Complaint;
- c. An award of punitive damages for Defendants’ intentional and/or reckless acts under Count II of the Complaint.
- d. Injunctive relief prohibiting Defendants from accessing Tech Systems’ computer systems or contacting Tech Systems’ offices, its employees, owners, vendors, or customers;
- e. An award of punitive damages in an amount to be determined at trial;
- f. An award of prejudgment interest according to law;
- g. An award of Plaintiff’s attorneys’ fees in this action;

- h. An award of Plaintiff's costs and expenses in this action; and
- i. An award or any other relief that this Court may deem just and proper.

Dated: Vienna, Virginia
April 4, 2012

Respectfully submitted,



Eric S. Crusius (VA Bar No. 77860)
Centre Law Group, LLC
Attorneys for Plaintiff
1953 Gallows Road, Suite 650
Vienna, Virginia 22182
Telephone: (703) 288-2800
Facsimile: (703) 288-4868